SISTEMA ELETRÔNICO DE VOTAÇÃO

| Perguntas mais frequentes |

3ª edição

Brasília – 2018

SISTEMA ELETRÔNICO DE VOTAÇÃO

| Perguntas mais frequentes |

3ª edição

Brasília – 2018

Secretaria de Gestão da Informação
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70070-600
Telefone: (61) 3030-9225

Secretário-Geral da Presidência
Estêvão Waterloo

Diretor-Geral
Rodrigo Curado Fleury

Secretária de Gestão da Informação
Janeth Aparecida Dias de Melo

Coordenadora de Editoração e Publicações
Renata Leite Motta Paes Medeiros

Unidade responsável pelo conteúdo
Secretaria de Tecnologia da Informação

Produção editorial e diagramação
Seção de Editoração e Programação Visual (Seprov/Cedip/SGI)

Capa e projeto gráfico
Verônica Estácio

Revisão
Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGI)
Harrison da Rocha e Vanda Tourinho

Impressão e acabamento
Seção de Serviços Gráficos (Segraf/Cedip/SGI)

Dados Internacionais de Catalogação na Publicação (CIP)
(Tribunal Superior Eleitoral – Biblioteca Professor Alysson Darowish Mitraud)

Brasil. Tribunal Superior Eleitoral.
Sistema eletrônico de votação : perguntas mais frequentes / Tribunal Superior Eleitoral. – 3. ed. – Brasília : Tribunal Superior Eleitoral, 2018.
35 p. ; 21 cm.

Unidade responsável pelo conteúdo: Secretaria de Tecnologia da Informação.

1. Segurança do voto na urna eletrônica – Brasil. 2. Voto eletrônico – Brasil. 3. Urna eletrônica – Brasil. 4. Registro digital do voto – Brasil. I. Título.

CDD 342.810 75
CDU 342.843.5(81)

Apresentação

Com o objetivo de fornecer esclarecimentos sobre as diversas questões e teorias difundidas pelos meios de comunicação acerca da segurança do processo eleitoral brasileiro, muitas vezes sem qualquer respaldo técnico ou legal, o Tribunal Superior Eleitoral compilou neste documento as perguntas mais frequentes a fim de que o cidadão conheça melhor os mecanismos adotados pela Justiça Eleitoral para trazer segurança e, consequentemente, confiança às eleições informatizadas do Brasil.

Sumário

1) Como o eleitor pode ter certeza de que a urna eletrônica é segura?

A urna eletrônica conta com diversos mecanismos por meio dos quais o próprio eleitor ou as entidades da sociedade civil podem verificar a segurança e o funcionamento do sistema de votação.

A Justiça Eleitoral utiliza o que há de mais moderno em termos de segurança da informação para garantir a integridade, a autenticidade e, quando necessário, o sigilo. Esses mecanismos foram postos à prova durante os Testes Públicos de Segurança, nos quais se mostraram robustos e foram aprimorados a partir da contribuição da comunidade técnica especializada. Além disso, há diversos mecanismos de auditoria e de verificação dos resultados que podem ser efetuados pelos candidatos, pelas coligações, pelo Ministério Público, pela Ordem dos Advogados do Brasil, pela Polícia Federal – dentre outras entidades – e também pelo próprio eleitor.

Um dos procedimentos de segurança que pode ser acompanhado pelo próprio eleitor é a cerimônia de votação paralela. Na véspera da eleição, em audiência pública, são sorteadas urnas para verificação. Estas urnas, que já estavam instaladas nos locais de votação, são, então, conduzidas ao Tribunal Regional Eleitoral e substituídas por outras, preparadas com o mesmo procedimento das originais. No dia da votação, em cerimônia pública, as urnas sorteadas são submetidas à votação, nas mesmas condições em que ocorreria na seção eleitoral, mas com o registro, em paralelo, dos votos que são depositados na urna eletrônica. Cada voto é registrado numa cédula de papel e, em seguida, replicado na urna eletrônica, tudo isso registrado em vídeo. Ao final do dia,

no mesmo horário em que se encerra a votação, são feitas a apuração das cédulas de papel e a comparação do resultado com o boletim da urna. Esse é um procedimento de fácil compreensão, cujo acompanhamento é bastante simples.

Outro mecanismo bastante simples de verificação é a conferência do Boletim de Urna (BU). Ao final da votação, o BU, com a apuração dos votos de uma seção, é documento público. O resultado de cada boletim pode ser facilmente confrontado com aquele publicado pelo Tribunal Superior Eleitoral na internet, seja pela conferência do resultado de cada seção eleitoral, seja pela conferência do resultado da totalização final. Esse procedimento, há muito tempo amplamente realizado pelos partidos políticos e pelas coligações, também pode ser feito pelo eleitor.

2) Como funciona a segurança da urna eletrônica? É possível executar aplicativos não autorizados na urna?

A urna eletrônica utiliza o que há de mais moderno quanto às tecnologias de criptografia, assinatura digital e resumo digital. Toda essa tecnologia é utilizada pelo *hardware* e pelo *software* da urna eletrônica para criar uma cadeia de confiança, garantindo que somente o *software* desenvolvido pelo Tribunal Superior Eleitoral (TSE), gerado durante a cerimônia de lacração dos sistemas eleitorais, possa ser executado nas urnas eletrônicas devidamente certificadas pela Justiça Eleitoral. Qualquer tentativa de executar *software* não autorizado na urna eletrônica resultará no bloqueio do seu funcionamento. De igual modo, tentativas de executar o *software* oficial num *hardware* não certificado implicam cancelamento da execução do aplicativo. Toda essa tecnologia tem sido exercitada durante os Testes Públicos de Segurança, o que tem permitido ao TSE tornar esses mecanismos cada vez mais seguros.

Para todo o conjunto de *software* produzido durante a cerimônia de lacração dos sistemas eleitorais são gerados assinaturas e resumos digitais. Caso haja qualquer suspeição quanto à autenticidade do *software* da urna eletrônica, as assinaturas digitais e os resumos digitais podem ser conferidos e validados, tanto por aplicativos desenvolvidos pelo TSE quanto por *software* desenvolvido pelos partidos políticos, pelo Ministério Público, pela Ordem dos Advogados do Brasil ou por outras entidades.

Além disso, todos os dados que alimentam a urna eletrônica assim como todos os resultados produzidos são protegidos por

assinatura digital. Não é possível modificar os dados de candidatos e de eleitores presentes na urna, por exemplo. Da mesma forma, não é possível modificar o resultado da votação contido no BU, o registro das operações feitas pelo *software* (*log*) e o arquivo de Registro Digital do Voto (RDV), dentre outros arquivos produzidos pela urna, uma vez que todos também estão protegidos pela assinatura digital.

Por fim, não é possível executar aplicativos não autorizados na urna eletrônica, tampouco modificar algum aplicativo da urna.

3) A urna eletrônica é vulnerável a ataques externos?

A urna eletrônica não é vulnerável a ataques externos. Ela é um equipamento que funciona de forma isolada, ou seja, não possui nenhum mecanismo que possibilite sua conexão a redes de computadores, como a internet. Além disso, não possui o *hardware* necessário para se conectar a uma rede ou mesmo a qualquer forma de conexão com ou sem fio. Vale destacar que o sistema operacional Linux contido na urna é preparado pela Justiça Eleitoral de forma a não incluir nenhum mecanismo de *software* que permita a conexão com redes ou o acesso remoto.

Ademais, as mídias utilizadas pela Justiça Eleitoral para a preparação da urna e gravação dos resultados são protegidas por técnicas modernas de assinatura digital. Não é possível a um atacante modificar qualquer arquivo presente nessas mídias.

4) Como o TSE controla/fiscaliza possíveis violações por pessoas que trabalham para a Justiça Eleitoral?

A Justiça Eleitoral utiliza ferramentas modernas de controle de versão do código-fonte dos sistemas eleitorais. A partir dessas ferramentas, é possível acompanhar toda modificação feita sobre o código-fonte, o que foi modificado e por quem. Somente grupo restrito de servidores e de colaboradores do Tribunal Superior Eleitoral tem acesso ao repositório de código-fonte e está autorizado a fazer modificações no *software*. Por isso, o *software* utilizado nas eleições é o mesmo em todo o Brasil e está sob controle estrito do Tribunal Superior Eleitoral.

De outra forma, o conhecimento sobre os sistemas eleitorais é segregado dentro do TSE. Isso significa que a equipe responsável pelo *software* da urna não é a mesma que cuida do sistema de totalização. Esse controle de acesso ocorre inclusive em nível de sistema de controle de versões. A quantidade de sistemas eleitorais envolvidos na realização de uma eleição é tão grande que se torna impraticável a um agente interno ter grau de conhecimento do todo que lhe permita realizar algum tipo de ataque.

Ademais, durante o período de desenvolvimento dos sistemas eleitorais, são realizados diversos testes tanto pelo TSE quanto pelos Tribunais Regionais, com o objetivo de averiguar o correto funcionamento de todo o conjunto de *software*. Os partidos políticos, o Ministério Público, a Ordem dos Advogados do Brasil, a Polícia Federal e outras entidades podem acompanhar o desenvolvimento do *software*

por meio da inspeção do código-fonte, no próprio ambiente no qual serão gerados os aplicativos utilizados nas eleições.

Além dos servidores do quadro da Justiça Eleitoral, são contratados, durante o período eleitoral, colaboradores para a prestação de apoio às atividades de transporte, preparação e manutenção das urnas eletrônicas. Também são convocados milhares de mesários para o dia da votação. Em nenhum momento, esses colaboradores ou os mesários possuem acesso ao código-fonte dos sistemas eleitorais. Embora essas pessoas tenham contato com as urnas eletrônicas, elas são incapazes de violar o *software* e o *hardware*. Isso é garantido pelos diversos mecanismos de segurança, baseados em assinatura digital e em criptografia, que criam cadeia de confiança entre *hardware* e *software* e impedem qualquer violação da urna eletrônica.

5) Desde a implantação da urna eletrônica, quantos e quais são os casos de suspeita de fraude identificados pelo TSE?

A urna eletrônica foi implantada nas eleições brasileiras de 1996. Nestes 22 anos, são frequentes os casos de suspeita de fraude. No entanto, nenhum caso até hoje foi identificado e comprovado. Essa conclusão é do TSE e também de outros órgãos que, constitucionalmente, têm a prerrogativa de investigar o processo eleitoral brasileiro e já realizaram auditorias independentes na urna eletrônica, como o Ministério Público e a Polícia Federal.

Em 2014 o partido do candidato derrotado na eleição presidencial conduziu extenso trabalho de auditoria das eleições daquele ano. Foram fornecidos os resultados de todas as urnas do país. A equipe do partido também teve acesso direto a urnas e a outros materiais das seções eleitorais. Após seis meses de trabalho, a conclusão da equipe do partido foi de que o resultado da eleição correspondia fielmente aos resultados apurados em todas as urnas, ou seja, não houve fraude na totalização dos votos.

Na verdade, a informatização do processo eleitoral brasileiro conseguiu eliminar uma série de manobras e desvios responsáveis por muitas fraudes nas eleições. Desde o cadastro único computadorizado de eleitores, em 1985, até a adoção do reconhecimento biométrico do eleitor, são inúmeros os mecanismos de combate à fraude que a Justiça Eleitoral vem adotando.

6) Por que o modelo de urna utilizado no Brasil não foi adotado em outros países?

O Brasil não trabalha com modelo de urna eletrônica que esteja disponível no mercado. A urna eletrônica brasileira é projeto único, desenvolvido para atender à realidade nacional, não se tratando de produto destinado à exportação.

Desde o advento da urna eletrônica, em 1996, diversos países têm consultado o Tribunal Superior Eleitoral com o objetivo de conhecer e adotar essa inovadora tecnologia brasileira. Em alguns casos, parcerias foram firmadas com o propósito de compartilhar conhecimento entre as nações. A partir de então, o voto eletrônico tem sido adotado por muitos países e, naturalmente, cada nação tem feito as adequações tecnológicas necessárias para compatibilizar a tecnologia com sua legislação, cultura e economia.

As parcerias firmadas no passado com outros países incluíram o empréstimo de urnas eletrônicas e as adequações de *software* necessárias para atender à legislação do país parceiro. Na prática, o TSE foi o responsável por todo o suporte de *software* e de *hardware* das eleições desses países, tudo devidamente acompanhado e fiscalizado pelas autoridades locais. Infelizmente, restrições orçamentárias e de pessoal forçaram o Tribunal Superior Eleitoral a encerrar essas parcerias e, a partir daí, alguns países não foram capazes de desenvolver tecnologia própria e abdicaram do voto eletrônico.

Outros países, após a troca de experiências com o TSE, desenvolveram sistemas informatizados próprios ou julgaram que o voto eletrônico possuía custo muito elevado de implantação – em locais onde a incidência de fraudes eleitorais é muito baixa ou a quantidade de eleitores é reduzida, o custo de adoção do voto eletrônico pode ser proibitivo. Atualmente, diversos países utilizam o voto eletrônico com regularidade, total ou parcialmente, e outros ainda estão testando e desenvolvendo soluções próprias.

7) O que é o Registro Digital do Voto (RDV)?

O RDV é o arquivo no qual os votos dos eleitores são registrados na urna. É a partir desse arquivo que é emitido o relatório zerésima – que indica que a urna não possui votos registrados. Também, com base no RDV, é gerado o Boletim de Urna (BU) – relatório com a apuração dos votos da seção.

O arquivo de RDV possui duas características importantes:

- **o voto é registrado exatamente como digitado pelo eleitor**: o RDV registra exatamente aquilo que foi digitado pelo eleitor na urna – e somente isso – sem nenhum processamento ou informação adicional (não há como vincular um voto no RDV a um eleitor). O RDV é utilizado somente no encerramento da votação para gerar o BU e, assim, realizar o somatório dos votos de cada candidato ou legenda e o cômputo de votos nulos e brancos. Como o RDV preserva exatamente aquilo que o eleitor digitou, esse arquivo é um instrumento importante de auditoria e de verificação da correta apuração de uma seção; e
- **o registro do voto garante seu sigilo**: assim como numa urna de lona tradicional, na qual as cédulas de papel ficam embaralhadas, impossibilitando a vinculação de cada cédula a um eleitor, no RDV cada voto é gravado numa posição aleatória do arquivo. Em particular, o voto, em cada cargo, é armazenado numa posição diferente, não permitindo nenhum tipo de associação entre

votos, tampouco a associação desses votos com a sequência de comparecimento dos eleitores.

Aos partidos políticos e às coligações é permitida a obtenção de cópias dos arquivos de RDV de todas as urnas que julgarem necessárias. De posse do RDV e da especificação do formato do arquivo, disponibilizada pela Justiça Eleitoral, os partidos e as coligações desenvolvem aplicativos próprios para comparação da apuração oficial da urna eletrônica com aquela produzida pelo seu próprio *software*.

8) Por que o voto não é impresso? A Justiça Eleitoral está descumprindo a lei?

O voto impresso foi instituído pela Lei nº 13.165/2015. Embora a lei previsse sua implantação a partir das Eleições 2018, o Supremo Tribunal Federal decidiu pela não implantação desse dispositivo até que seja julgada a constitucionalidade da impressão de votos. Com isso, a Justiça Eleitoral está impedida de implantar o voto impresso no momento.

Os propósitos do voto impresso são:

- melhorar a capacidade de auditoria e permitir a recontagem de votos; e
- permitir que o eleitor comprove se o voto manifestado por ele é o mesmo que chegou ao TSE para totalização.

No caso da auditoria, a partir de amostragem das urnas, os votos em papel seriam apurados e comparados com o resultado apresentado pela urna eletrônica. Parte-se do princípio de que o total dos votos impressos é mais confiável que o total da urna eletrônica, uma vez que teria sido conferido pelo eleitor.

De outro modo, devido à intervenção manual direta, a possibilidade de fraude com relação ao papel é grande, o que acarretaria resultados divergentes e menos confiáveis que o da própria urna eletrônica. Na prática, o que se vislumbra é que o alvo de ataques seja deslocado da urna eletrônica para o seu processo de auditoria por contagem dos votos impressos, o que pode implicar a anulação indevida de votos ou até

mesmo a convocação de novas eleições num cenário em que a vontade do eleitor esteja perfeitamente íntegra nos registros eletrônicos.

Assim como o voto evoluiu do papel para o meio eletrônico também é preciso que os processos de auditoria evoluam. Existem outras formas de auditoria mais baratas e seguras do que o uso do voto impresso. A Justiça Eleitoral, inclusive, já faz uso delas, como a votação paralela e a apresentação do código-fonte nos seis meses que antecedem o fechamento do *software* para uso nas eleições. E o próprio arquivo de RDV é instrumento de auditoria importante, já utilizado pelos partidos e pelas coligações para verificação da integridade da apuração da urna eletrônica.

Com relação à comprovação pelo eleitor de seu próprio voto, essa possibilidade viola o sigilo do voto, que é uma garantia expressa pela Constituição, uma vez que o eleitor poderá apresentar prova do seu voto a outra pessoa. Mesmo com registro impresso do voto, o eleitor nunca poderá ter a garantia de que seu voto foi efetivamente contado num processo de auditoria.

Desde a aprovação da Lei nº 13.165/2015, o Tribunal Superior Eleitoral conduziu todos os esforços necessários para a implantação do voto impresso a partir das Eleições 2018: a regulamentação da lei foi elaborada, discutida e aprovada; as alterações no *software* da urna foram desenvolvidas; e uma empresa foi contratada por licitação para o fornecimento das impressoras de votos.

9) O sistema da urna eletrônica mantém registro das suas operações?

A urna eletrônica mantém arquivo com o registro cronológico das principais operações realizadas pelo seu *software* – esse é o arquivo de *log*. Dentre outras operações, ficam registrados, nesse arquivo, o início e o encerramento da votação, a emissão de relatórios, os aplicativos que foram executados, os ajustes de data e hora, a realização de procedimentos de contingência e os registros que auxiliam na avaliação da dinâmica do voto.

O arquivo de *log* é mais um mecanismo de transparência e de auditoria disponibilizado pela Justiça Eleitoral. A partir do *log*, é possível analisar toda a história da urna eletrônica desde a sua preparação até o encerramento da votação no segundo turno. Assim como o arquivo de RDV, o arquivo de *log* também é disponibilizado aos partidos políticos e às coligações, para que estes façam sua própria análise dos eventos ocorridos na urna eletrônica.

A partir dos arquivos de *log* de todas as urnas eletrônicas, o Tribunal Superior Eleitoral monta poderoso banco de dados, do qual é possível extrair informações valiosas sobre a dinâmica da votação. Essas informações subsidiam a melhoria de diversos processos relacionados à urna eletrônica, tais como a preparação da urna, os componentes que estão apresentando maior taxa de defeitos, a velocidade da votação e a dinâmica da utilização da biometria. Tudo isso é utilizado para prover melhor atendimento ao eleitor no dia da votação e para agilizar os trabalhos de preparação e fiscalização das urnas eletrônicas.

10) Qual a finalidade de o sistema da urna eletrônica armazenar a hora de votação?

A urna eletrônica armazena a hora em que um eleitor foi habilitado para votar, sem identificá-lo. Essa informação é útil para o cálculo de indicadores gerenciais, como o tempo médio de votação do eleitor. Com base nessa informação, é possível, por exemplo, realizar análise sobre a quantidade de eleitores por seção, permitindo à Justiça Eleitoral ajustar esse número a fim de reduzir a ocorrência de filas, de modo que o eleitor vote com tranquilidade.

11) O que são os Testes Públicos de Segurança?

Os Testes Públicos de Segurança têm por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos, além de propiciar melhorias no processo eleitoral. Nesse sentido, o TSE editou, em 2015, a Resolução nº 23.444, dispondo que os Testes Públicos de Segurança constituem parte integrante do processo eleitoral brasileiro e serão realizados antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

Ao abrir os sistemas para inspeção dos códigos-fonte e para os exercícios diversos, a Justiça Eleitoral busca encontrar oportunidades de aprimoramento dos mecanismos de segurança do *software*, contando com a visão e com a experiência de outros órgãos públicos, de estudiosos e de qualquer cidadão interessado.

Os Testes Públicos de Segurança são utilizados pelo TSE como instrumento auxiliar para a melhoria contínua dos sistemas eleitorais, não havendo interesse da Justiça Eleitoral em promover qualquer tipo de competição ou promoção individual dos participantes.

12) A falha encontrada no embaralhamento dos votos em 2012 compromete a integridade dos resultados? Ela já foi corrigida?

A falha encontrada no Teste Público de Segurança realizado em 2012 estava relacionada ao algoritmo de embaralhamento dos votos no RDV, ou seja, à ordem de gravação dos votos de cada eleitor. De nenhuma forma, a contagem dos votos é afetada, portanto o resultado é íntegro.

Para corrigir a não conformidade encontrada e inviabilizar o reordenamento dos votos, o algoritmo foi modificado e aprimorado imediatamente após a descoberta do problema. Visando certificar a qualidade do novo algoritmo, inúmeros testes foram realizados exaustivamente, todos baseados em técnicas utilizadas internacionalmente. Uma dessas técnicas é o DieHard, um teste de aleatoriedade que verifica a efetividade do embaralhamento de sequências. Também foram utilizadas regras estabelecidas pelo National Institute of Standards and Technology .

A solução implementada foi aberta a amplo escrutínio, inclusive nas edições de 2016 e de 2017 dos Testes Públicos de Segurança. O *software* atual se mostrou robusto e não foi mais alvo de ataques.

13) As falhas encontradas em 2017 já foram corrigidas?

Todas as falhas encontradas nos Testes Públicos de Segurança de 2017 já foram corrigidas. O Tribunal Superior Eleitoral deu total transparência aos achados dos investigadores, publicando relatório detalhado em http://www.tse.jus.br/hotsites/teste-publico-seguranca-2017/arquivos/tps2017-relatoriotecnico.pdf. Em maio de 2018, os investigadores foram convidados a verificar a efetividade das correções implementadas no *software* e a conclusão foi de que tudo está corrigido. A equipe técnica do TSE também deu total transparência às correções efetuadas em relatório publicado em http://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017-1527192798117.

A realização periódica dos Testes Públicos de Segurança tem se mostrado grande sucesso, na medida em que a comunidade técnica especializada tem ajudado efetivamente a equipe técnica do Tribunal Superior Eleitoral a desenvolver sistemas cada vez mais seguros para as eleições.

14) O código-fonte do *Software* de Votação pode ser aberto à comunidade?

Atualmente, já é permitido aos representantes técnicos dos partidos políticos, ao Ministério Público, à Ordem dos Advogados do Brasil, à Polícia Federal, dentre outras entidades, o acesso ao código-fonte do *Software* de Votação e de todo o conjunto de *software* da urna eletrônica. Portanto, já existe transparência sobre o código-fonte. Naturalmente, o Tribunal Superior Eleitoral estuda ampliar ainda mais o acesso ao código-fonte para que mais pessoas e instituições possam verificar a correção e lisura do *software*.

15) É possível dizer que a urna brasileira é de primeira geração? As ditas urnas de segunda e terceira gerações são mais seguras?

A urna eletrônica brasileira é equipamento inovador e foi introduzido no processo eleitoral em 1996. Todo o projeto de *hardware* e de *software* da urna é conduzido pelo Tribunal Superior Eleitoral, que tem contado com o apoio de membros da academia desde sua concepção até as mais recentes evoluções realizadas. Trata-se, portanto, de projeto desenvolvido completamente no Brasil que passa por constante evolução, cuja fabricação, por delegação do TSE, fica a cargo de uma empresa contratada por licitação.

A denominação de “gerações” de urnas, comumente utilizada como estratégia de mercado para a venda de equipamentos mais novos, geralmente está associada ao modo de operação do sistema: registro totalmente eletrônico, tal como feito pela urna brasileira, registro material que é digitalizado (registro em papel é submetido a um *scanner*, por exemplo) ou registro digitalizado que é materializado (o equipamento imprime registro do voto, por exemplo), sendo as duas últimas associadas à “segunda geração”. Esses diversos modos de operação foram empregados em vários momentos, por diferentes países e com tecnologias distintas, não sendo possível traçar linha evolutiva entre eles, tampouco se pode afirmar que determinado modelo é mais ou menos seguro que outro. Além disso, a materialização do voto em papel abre brechas para que esse instrumento de auditoria seja atacado, tal como já ocorria antes do voto eletrônico.

A chamada "terceira geração" fornece ao eleitor mecanismo de verificação quanto à inclusão do seu voto no sistema de totalização. Caso o mecanismo não inclua alguma forma que preserve o sigilo do voto, inclusive para o próprio eleitor, este poderá ser coagido a votar e a entregar o comprovante ao criminoso. Além disso, se ao eleitor somente é permitido verificar se o seu voto foi contabilizado com a utilização de sistema informatizado, recai-se sobre o mesmo problema de confiança exclusiva no *software*, tão criticado na "primeira geração".

A urna eletrônica brasileira é um projeto com foco em segurança de *hardware* e de *software* que conta com diversos mecanismos de auditoria. Trata-se de produto moderno e em constante aprimoramento, com processo evolutivo próprio. Ao longo dos últimos anos, foram incluídos leitores biométricos, mídias de armazenamento e processadores de maior capacidade e confiabilidade bem como *hardware* criptográfico. Com efeito, todos esses avanços incrementam substancialmente a confiabilidade e a segurança do voto eletrônico.

16) O que é o aplicativo Ajuste de Data e Hora (ADH)? É possível utilizá-lo para fraudar os votos de uma urna?

O aplicativo ADH faz parte da instalação da urna eletrônica e é utilizado para efetuar ajustes no relógio da urna. É utilizado em situações em que o operador informou data e hora incorretas durante a preparação da urna para a eleição. Ele também é utilizado nos casos em que o relógio da urna apresenta algum problema de bateria e passa a apresentar hora incorreta. Não é possível utilizar o ADH para fraudar os votos de uma urna.

É importante que o relógio da urna esteja com a data e hora corretas, pois algumas operações são controladas em função disso, tais como:

- liberação da emissão da zerésima, a partir das 7h do dia da votação;
- liberação para habilitação de eleitores, a partir das 8h do dia da votação; e
- liberação para encerramento da votação, a partir das 17h do dia da votação.

Não é possível utilizar o ADH para realizar qualquer tipo de fraude na urna eletrônica. Apesar disso, tem sido alardeado recentemente que possível fraude envolveria o uso do ADH. O ataque ocorreria da seguinte forma:

- o atacante tem acesso a uma urna preparada para a eleição antes do dia da votação e a uma mídia de ativação do ADH;
- utiliza-se o ADH para adiantar o relógio da urna até o dia e hora de início da votação;
- faz-se a inserção de votos espúrios na urna até o horário de encerramento;
- retira-se a mídia com o resultado espúrio, e esta é guardada até o dia da votação;
- novamente utiliza-se o ADH para ajustar o relógio da urna com a data e hora reais, outra mídia vazia para a gravação dos resultados é inserida na urna e seu compartimento é lacrado;
- no dia da votação, na seção eleitoral, essa urna coletaria os votos reais normalmente, porém, ao final da votação, em vez de encaminhar para transmissão dos resultados a mídia utilizada na seção eleitoral, utiliza-se a mídia com os votos espúrios gerados com antecedência.

Em resumo, a hipótese apresentada é que o controle para início da captação de votos está sustentado somente na data e hora atuais. Ocorre que isso não é verdade.

O *Software* de Votação mantém o último estado de sua execução. Isso significa que, uma vez encerrada a votação, há bloqueio no *software* da urna que impede a captação de votos até que esta seja preparada para o segundo turno, ou seja, preparada para nova eleição. Além disso, em nenhum momento, o *Software* de Votação apaga ou reinicia os registros contidos no arquivo de RDV que contém cada voto inserido na urna. É a partir do RDV que o *software* emite o relatório zerésima, indicando que não há votos presentes na urna.

Por último, mesmo que houvesse troca de mídias e tivessem sido gerados dois resultados diferentes, o registro impresso pelo Boletim de Urna na seção não coincidiria com aquele recebido pela totalização. Facilmente os fiscais de partido – e qualquer cidadão, na verdade – poderiam confrontar o resultado apurado para uma seção pela totalização oficial com aquele que foi publicado na seção eleitoral, sendo que este último retrata o resultado real e correto.

17) Existe mesmo chave única que protege todas as mídias das urnas? De posse dessa chave, seria possível adulterar o conteúdo das mídias?

Parte das mídias utilizadas nas urnas utiliza mecanismo geral para ocultação das informações, que é a criptografia do sistema de arquivos. As mídias em questão são os cartões de memória da urna (interno e externo), nos quais estão gravados o sistema operacional e os aplicativos (cartão interno), os dados de eleitores e de candidatos e os resultados da votação (duplicados nos cartões interno e externo).

O objetivo da criptografia do sistema de arquivos é impor barreira adicional a um atacante externo com pouco ou nenhum conhecimento sobre a organização do *software* da urna. Dessa forma, um possível atacante encontraria dificuldades em iniciar análise do conteúdo das mídias.

Existe chave única utilizada pela criptografia do sistema de arquivos de todos os cartões de memória. Se essa chave não fosse única, seria impraticável realizar procedimentos de contingência – substituir uma urna defeituosa por outra em perfeito estado, permitindo que a votação continue do mesmo ponto em que foi interrompida. Além disso, se a chave não fosse única, qualquer auditoria sobre as urnas estaria comprometida. No entanto, é incorreto afirmar que, a partir da posse da chave do sistema de arquivos, é possível gerar mídias “de diferente teor”.

É importante destacar que a criptografia do sistema de arquivos não é o mecanismo no qual se sustenta toda a segurança do *software* da urna.

Na verdade, todos os arquivos que requerem integridade e autenticidade são assinados digitalmente. Esse é o caso, por exemplo, dos aplicativos da urna e dos arquivos de dados de eleitores e de candidatos, assim como do Boletim de Urna e do registro digital do voto, dentre outros. Além disso, os arquivos que requerem sigilo são criptografados. Em todos esses casos, são utilizadas chaves diversas. Esses mecanismos de assinatura e de criptografia impedem que o conteúdo das mídias seja adulterado.

18) A empresa Smartmatic fabrica as urnas brasileiras e cuida de todo o processo eleitoral?

A urna eletrônica brasileira nunca foi fabricada pela Smartmatic. Na sua concepção, entre os anos de 1995 e 1996, a elaboração do projeto técnico de *hardware* e de *software* da urna foi realizada por grupo de trabalho composto por especialistas em informática, eletrônica e comunicações. Desse feito participaram integrantes da Justiça Eleitoral, das Forças Armadas, do Ministério da Ciência e Tecnologia, do Instituto Tecnológico de Aeronáutica, do Instituto Nacional de Pesquisas Espaciais e do Ministério das Comunicações.

Desde então, a fabricação das urnas é de responsabilidade de empresas contratadas em processo licitatório, plenamente transparente e auditável. Em nenhuma ocasião, a Smartmatic foi vencedora dessa licitação.

Além disso, todo o *software* dos sistemas envolvidos nas eleições é desenvolvido pelas equipes do TSE. A operação desses sistemas, ou seja, a gestão de todo o processo eleitoral, é realizada exclusivamente por servidores do Tribunal Superior Eleitoral e dos Tribunais Regionais Eleitorais, não sendo delegado, em hipótese alguma, a empresas contratadas.